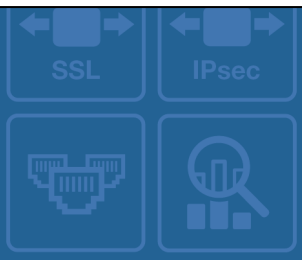
FORTINET

High Performance Network Security

# FortiMail™ Release Notes

VERSION 5.4.1 GA



**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

**FORTINET COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

October 13, 2017

# TABLE OF CONTENTS

# Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in this release.

## Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400C
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000C
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

# What's New

The following table summarizes the new features and enhancements in this release.

| Features | Descriptions |
|---|---|
| **SAML SSO** | Webmail SAML SSO support for FortiAuthenticator. |
| **Webmail themes** | In 5.4 and earlier, the webmail theme was static. FortiMail 5.4.1 introduces 3 themes in red, blue and green which can be configured by the administrator (System > Customization > Appearance > Webmail Portal > Default theme). If enabled in the configuration by the administrator, the user can also select their own theme (Preferences > Account Settings > Theme). |
| **Log view** | In 5.4 and earlier, the log views under Monitor > Log displays by default a list of log files sorted by start and end time with the most current at the top. In 5.4.1, the current log file is displayed by default. To view the full list of files, select the List button.<br>In the Antivirus log, a new filter option “Type” has been added to quickly switch the display from showing “all” logs to Infected, Malware Outbreak, File Signature or FortiSandbox. |

# What's Changed

The following table lists some of the changes in this release.

| Features | Descriptions |
| --- | --- |
| **Password policy** | Force admin users to change their passwords upon logon if their existing passwords do not comply with the configured password policy. |

# Special Notices

## TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

## Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

## Recommended browsers on desktop computers for administration and Webmail

- Internet Explorer 11 (Windows 7) and Edge (Windows 10)
- Firefox 52 to 54
- Safari 9 to 10 (Mac OS X)
- Google Chrome 53 to 59

## Recommended browsers on mobile devices for webmail access

- Official Safari browser for iOS 9 to10
- Official Google Chrome browser for Android 5 to 7

## FortiSandbox support

The current FortiMail release requires FortiSandbox 2.1 or newer releases. FortiSandbox 2.3 or new releases are highly recommended.

# Firmware Upgrade/Downgrade

## Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *Maintenance* > *System* > *Configuration*.
- After any firmware upgrade/downgrade:
  - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the web UI screens.
  - The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate AV signature update as soon as possible.

## Upgrade path

### For any 5.x release

Any 5.x release older than 5.2.3

↓

5.2.3 (Build 436)

↓

5.2.8 (Build 467)

↓

5.3.10 (Build 643)

↓

5.4.1 (Build 704)

### For any 4.x release

Any 4.x release older than 4.3.6

↓

4.3.6 (Build 540)

↓

5.2.3 (Build 436)

↓

5.2.8 (Build 467)

↓

5.3.10 (Build 643)

↓

5.4.1 (Build 704)

After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Dashboard* > *Status* on the Web UI.

# Firmware downgrade

## Downgrading from 5.4.1 to 5.x or 4.x releases

Downgrading from 5.4.1 release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 5.4.1 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

# Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

## Antivirus/Antispam/Content

| Bug ID | Description |
|---|---|
| 452514 | LDAP override of antispam/antivirus/content profiles does not work. |
| 451012 | Enabling terrorism in DLP may cause false positives. |
| 445141 | Antivirus does not work for associated domains. |
| 451741 | Custom email templates are lost after executing running the "execute formatmaildisk" command. |
| 444229 | Resource profiles of domain-level recipients policies are not applied on domain associates. |
| 448433 | When an email message is accepted for delivery, but get rejected due to some policies, the message should not be discarded. It should be sent to system quarantine. |
| 444305 | Email in HTML format cannot be caught by SSN Smart ID. |
| 443407 | System quarantine folder settings are ignored in antispam and content action profiles. |
| 444546 | FortiMail analysis is performed on URLs containing "(" or ")" parentheses. |
| 444394 | Under Security > Quarantine > Quarantine Control, the Quarantine Release Re-scan Settings not only performs antivirus but also antispam scanning. |
| 444040 | Only the first DLP scan rule recipient exception is honored when using multiple recipient exceptions. |
| 448996 | In domain settings, the custom quarantine report template (per domain) does not takes effect. |
| 448879 | Unable to release quarantined email using the search function. |
| 447735 | Part of email body is lost after converting from HTML to text by content filters. |
| 444961 | Unable to add domain names containing "_" (underscore) to block/safe lists. |
| 447474 | Korean words are not displayed properly in quarantine reports. |
| 453695 | Spam image scanning is too aggressive and causes false positives. |
| 452865 | Changing the value of personal quarantine retention period does not have effect. |

## MTA/Proxy

| Bug ID | Description |
|---|---|
| 444991 | User alias should not be treated as case-sensitive when receiving email. |
| 449760 | Sender address rate control (maximum recipients) is still enforced when not enabled. |
| 444989 | User alias does not allow the usage of ' (apostrophe). |

## System

| Bug ID | Description |
|---|---|
| 447713 | SSH port changes do not work. |
| 450163 | SSH service is not available after executing the command "exe formatmaildisk". |
| 444774 | Password policy does not work properly for administrators. |
| 442762 | Authserver security fails with plain auth in some cases. |
| 445861 | Migration of contacts from MiraMail does not work properly. |
| 263586 | All administrators should be able to manipulate the safe/block lists using the CLI. |
| 449016 | Attachment file names with S-JIS encode are garbled. |
| 399986 | When all admin users have trusted hosts configured, the admin login page should not be displayed any more. |
| 445295 | Archive rotation does not work properly and the inbox file in archive is deleted after system reboot. |
| 448818 | After enabling password policy and applying it to administrators under System > Configuration > Option, LDAP admin users cannot be created any more. |
| 444825 | After upgrading from 5.3 to 5.4, incoming disclaimers appear as attachments. |
| 451467 | In server mode, LDAP address book sharing to Outlook and Thunderbird stops working after upgrading to 5.4.0. |
| 453039 | When FortiMail host name is changed, the change is not reflected on the FortiSandbox GUI. |
| 453563 | System-level outgoing recipient policies break SMTP authentication. |

## Admin GUI/Webmail

| Bug ID | Description |
|---|---|
| 447976 | In webmail, when sending email to a recipient whose display name contains "." (dot), the "Invalid Email Address" error is returned when clicking Send. |
| 448978 | Chinese characters are used on webmail GUI even though the language is set to Japanese. |
| 445483 | The System Quarantine > Bulk > Current display no email when the filter is set to Unreleased. |
| 450988 | Under Monitor > Sender Reputation > Display, the Delete button does not work. |
| 448430 | In webmail, it is unable to save email whose subject is double byte (Japanese) and long. |
| 451740 | In webmail, when printing with the More > Print option, attachment file names are not printed. |
| 444994 | Ordering the system quarantine by size does not work properly. |
| 380258 | Webmail calendar does not display events correctly. |
| 443063 | Japanese characters are garbled in webmail. |
| 444068 | Internal server error occurs when saving attachments by using the "Save All" button. |

## CLI

| Bug ID | Description |
|---|---|
| 446045 | The CLI command to remove expired IBE users (execute ibe user clean-expired-user) does not work. |
| 444571 | Memory usage calculation in CLI command is incorrect. |

# Known Issues

The following table lists some minor known issues. .

| Bug ID | Description |
|---|---|
| 307919 | Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments. |
| 381511 | IBE messages are not signed with DKIM although DKIM signing is enabled. |

# Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

**Figure 1:** Customer Service & Support image checksum tool